Dissecting Leakage Resilient PRFs with Multivariate Localized EM Attacks

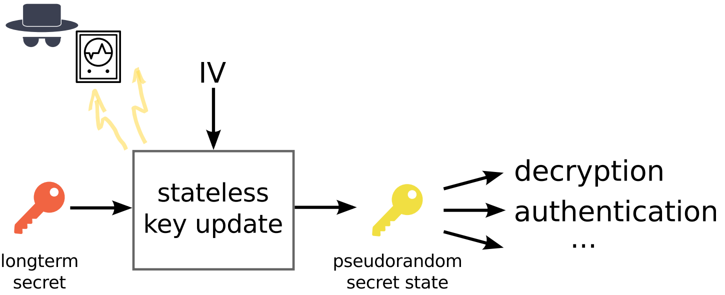
A Practical Security Evaluation on FPGA

Florian Unterstein Johann Heyszl Fabrizio De Santis[a] Robert Specht, 13.04.2017

[a]Technical University Munich

Motivation

- Stateless devices often need to derive a pseudorandom secret state from a long-term secret and public inputs
- Interaction between secret and public data needs to be protected against side-channel attacks

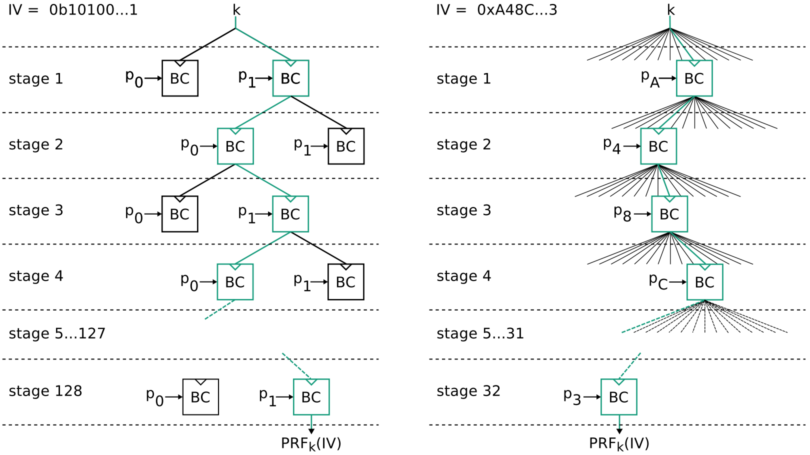


Motivation
Leakage Resilient Cryptography

- Aims to bound the leakage per execution such that an attacker cannot accumulate information endlessly
- Two important methods:
  - Limited data complexity, i.e. the number of different operations under one key
  - Algorithmic noise from parallel implementations with carefully chosen inputs

Motivation

Leakage Resilient Pseudo Random Functions



LR-PRF from Medwed et al. [3]

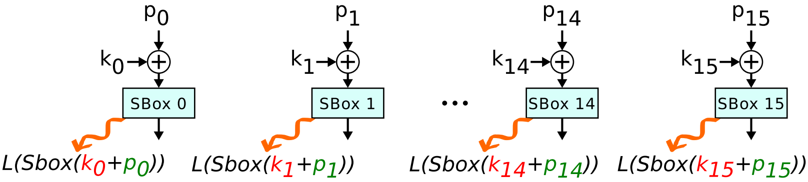
Motivation
Leakage Resilient Pseudo Random Functions

- It was shown that limited data complexity with random inputs is insecure [3]
- Instead, carefully chosen inputs and parallel hardware have been used
- Idea: All S-boxes work in parallel and public inputs to S-boxes are equal
- S-boxes working in parallel adds algorithmic noise
- Carefully chosen inputs prevents divide-and-conquer

Motivation

Leakage Resilient Pseudo Random Functions

- Typically: Attack key byte-by-byte and divide by known plaintext:



- Carefully chosen inputs: $p_0 = p_1 = \cdots = p_{14} = p_{15}$
- If all S-boxes leak in parallel at the same time, an attacker cannot differentiate between key bytes
- Even if all key bytes are recovered, the order remains unknown

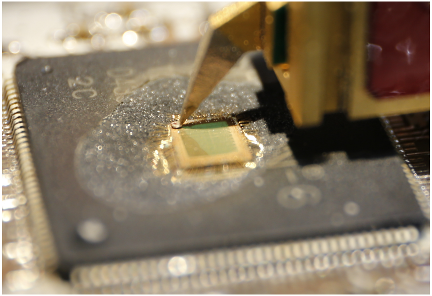
Motivation
Our Research Questions

- Are such constructions secure on FPGAs?
- Specifically:
  - Does parallelism with minimal data complexity hold against state-of-the-art localized electromagnetic measurements?
  - What security level can we reach against multivariate template attacks?
  - How does the S-box placement and routing affect the results?

  → Practical security evaluation on an FPGA device

Setup
Measurement Setup and DUT

- Measurement setup
  - **100 µm** diameter EM probe
  - **2.5 GHz** bandwidth oscilloscope
  - **5**GS/s sampling rate
- DUT
  - Xilinx Spartan 6 **45 nm** FPGA
  - **20 MHz** clock
  - Mounted on X-Y-table

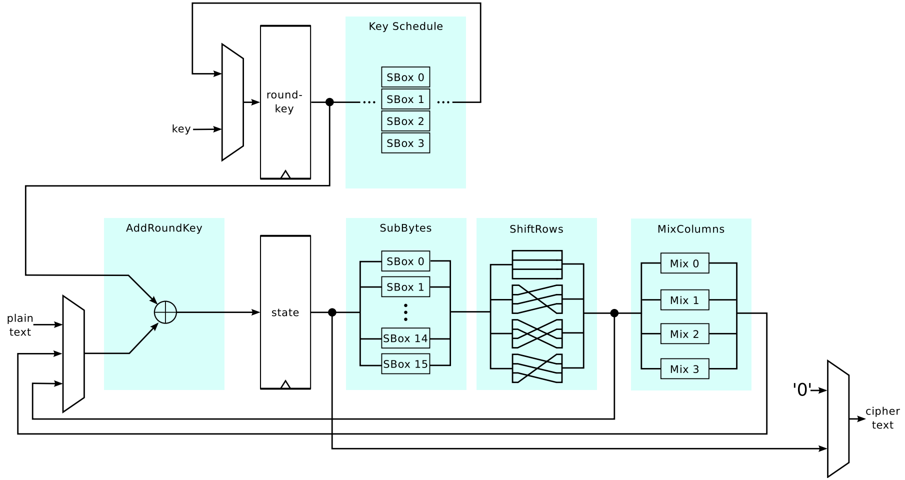


Setup
FPGA Designs

- We implemented a LR-PRF in two configurations:
  - Data complexity **16** per stage and **32** stages per evaluation
  - Data complexity **2** per stage and **128** stages per evaluation

- For each configuration, we implemented two versions with different placement:
  - Loose placement:
    Placement and routing is done without constraints, design is spread across the whole FPGA (about **7 mm**^{2})
  - Dense placement:
    All S-boxes are instantiated from a hard macro S-box with fixed internal structure and routing, the entire AES is constrained in a small area (about **0.5 mm**^{2})

Setup
AES Hardware Design

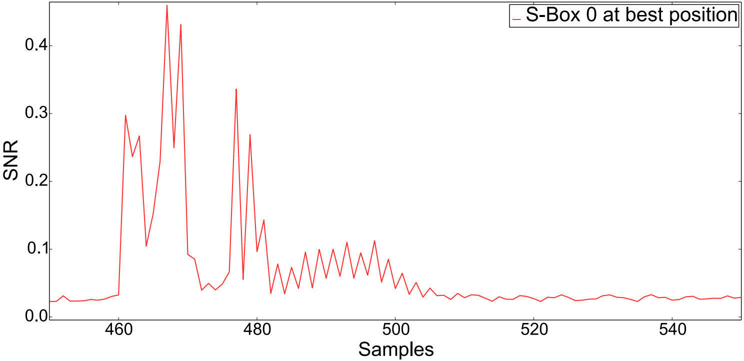


Analysis
Overview

1. Spatial localization of S-boxes
2. Profiling phase
3. Attack phase

Analysis
Step 1: Spatial Localization of S-boxes

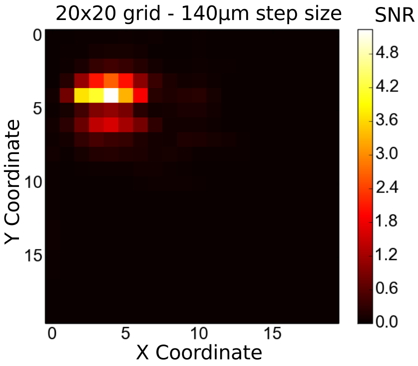
- Find positions with maximum leakage for each S-box
- Signal to Noise Ratio (SNR) of attacked values used as metric
- Hot spots for each S-box are clearly visible in all designs



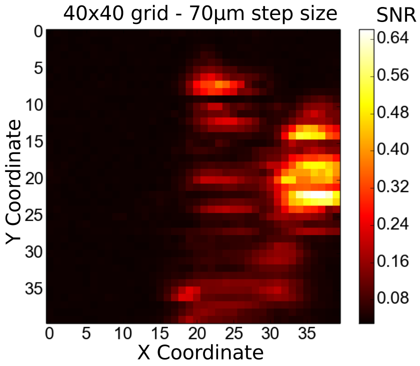
Fraunhofer AISEC

Analysis

Example: SNR for S-box 0 with different placements



(a) Loose placement



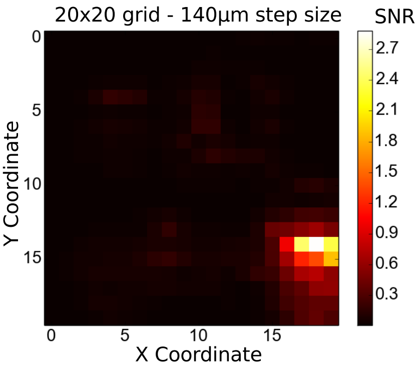
(b) Dense placement

- High relative SNR clearly visible
- Dense placement has lower leakage

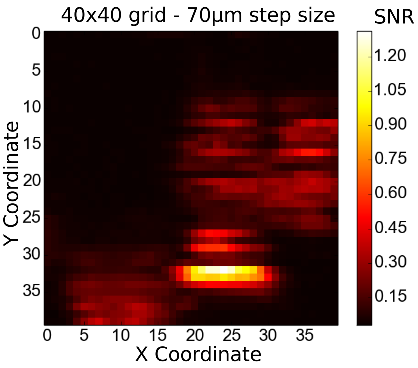
Fraunhofer AISEC

Analysis

Example: SNR for S-box 1 with different placements



(a) Loose placement



(b) Dense placement

- Different S-boxes give different locations with high SNR

Analysis
Step 2: Profiling Phase

- Take measurements at each S-box's derived position
- For each S-box:
  - Calculate Linear Discriminant Analysis (LDA) [1] transformation matrix to reduce the dimensionality
  - Build templates for each S-box input value in the LDA transformed subspace

Analysis
Step 3: Attack Phase

- Take new measurements at each S-box's derived position
- For each S-box:
  - Apply LDA transformation to reduce dimensionality
  - Match templates with each trace and calculate subkey probabilities
- Use key rank estimation to calculate guessing entropy of entire key [2] from the resulting subkey lists

Results

Estimated Key Ranks After the Attacks

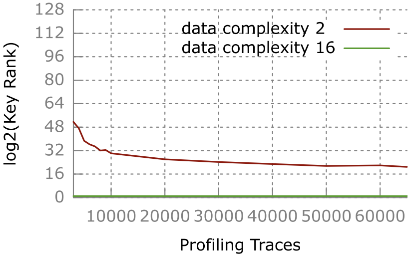
Data Complexity	S-Box Placement	Est. Key Rank
16	Loose	1
16	Dense	1
2	Loose	2^{20}
2	Dense	2^{48}

- Security level insufficient for all designs and configurations!
- Is this the lower bound or can we do better?

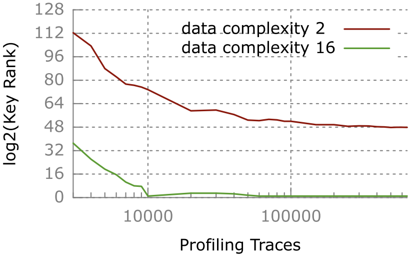
Fraunhofer AISEC

Results

Varying Number of Profiling Traces



(a) Loose design



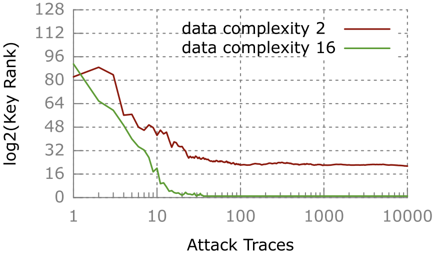
(b) Dense design

- Profiling is sufficient

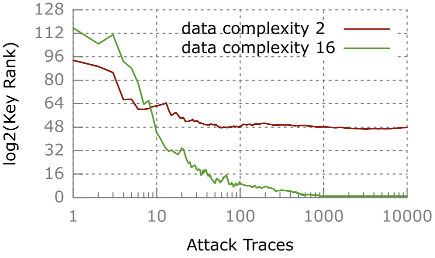
Fraunhofer AISEC

Results

Varying Number of Attack Traces



(a) Loose design



(b) Dense design

- Number of attack traces is sufficient
- Remaining entropy is lower bound for this implementation and DUT

Fraunhofer AISEC

Summary

- For implementing LR-PRFs on a **45 nm** FPGA we find that

1. Localized EM measurements together with LDA and multivariate template attacks are a big threat
2. For efficient PRFs with larger data complexity per stage the attack leads to full key recovery
3. For the minimum possible data complexity **2**, the remaining key entropy is still insufficient
4. While dense placement hinders the attack, it is still insufficient

Contact Information

Florian Unterstein

Department
Hardware Security

Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

Address: Parkring 4
85748 Garching (near Munich)
Germany
Internet: http://www.aisec.fraunhofer.de

Phone: +49 89 3229986-143
Fax: +49 89 3229986-222
E-Mail: forename.surname@aisec.fraunhofer.de

Fraunhofer AISEC

Bibliography

- Fisher, R.A.: The use of multiple measurements in taxonomic problems. Annals of Eugenics 7(7), 179–188 (1936)
- Glowacz, C., Grosso, V., Poussier, R., Schüth, J., Standaert, F.: Simpler and more efficient rank estimation for side-channel security assessment. In: Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers. pp. 117–129 (2015)
- Medwed, M., Standaert, F., Joux, A.: Towards super-exponential side-channel security with efficient leakage-resilient PRFs. In: Prouff, E., Schaumont, P. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7428, pp. 193–212. Springer (2012)

Backup

- Langer ICR HH 100-27 **100 µm** diameter EM probe
- Langer PA303 30 dB pre-amplifier
- LeCroy WavePro 725Zi oscilloscope with **2.5 GHz** bandwidth and 5 GS/s
- X-Y-table with step size of **140 µm** and **70 µm**
- Measurement positions are located within an area of about **2.8 mm** by **2.8 mm** between the bonding wires
- **45 nm** Xilinx Spartan **6** XC6SLX9-3TQG144C FPGA